PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-259569
(43)Date of publication of application : 22.09.2000

(51)Int.Cl. G06F 15/00
G06F 12/14
G06F 13/00

(21)Application number : 11-066666
(22)Date of filing : 12.03.1999

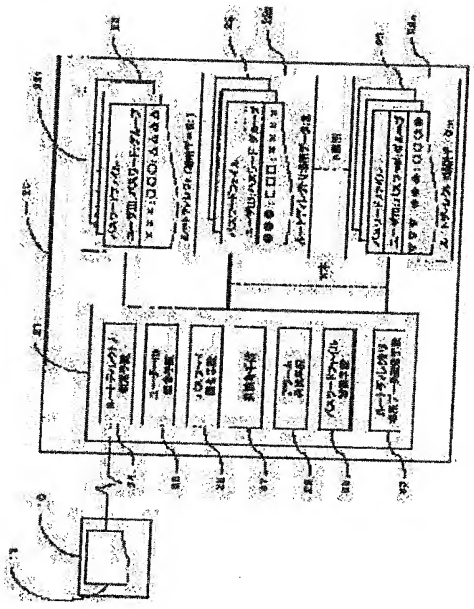
(71)Applicant : NEC ENG LTD
(72)Inventor : SHINKAWA YOSHIHIKO

(54) METHOD AND SYSTEM FOR CERTIFYING PASSWORD

(57)Abstract:

PROBLEM TO BE SOLVED: To block the illegal invasion of the third person to an information communication network system even when a password is stolen by the third person in the information network communication system.

SOLUTION: Inside a server 20, route directories 221-22n are prepared at plural spots for storing a password file 23 for each user. At the time of access, a user ID, a password and the place data of the route directory storing the password file 23 are transmitted to the server 20 and when a password recorded in the password file 23 of the relevant route directory is coincident with a password sent from an access terminal, log-in to the server 20 is permitted. At the same time, at the time of log-out, the place of the route directory storing the password file 23 is moved from the route directory stored up to the moment to the other route directory at random and the place data of that moved route directory are stored in a storage part 11 of an access terminal 10.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－259569
（P2000－259569A）
(43)公開日　平成12年９月22日(2000.9.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｂ	５Ｂ０１７
	12/14	３２０	12/14	３２０Ｃ	５Ｂ０８５
	13/00	３５１	13/00	３５１Ｚ	５Ｂ０８９

審査請求　未請求　請求項の数２　ＯＬ　（全８頁）

(21)出願番号　特願平11－66666

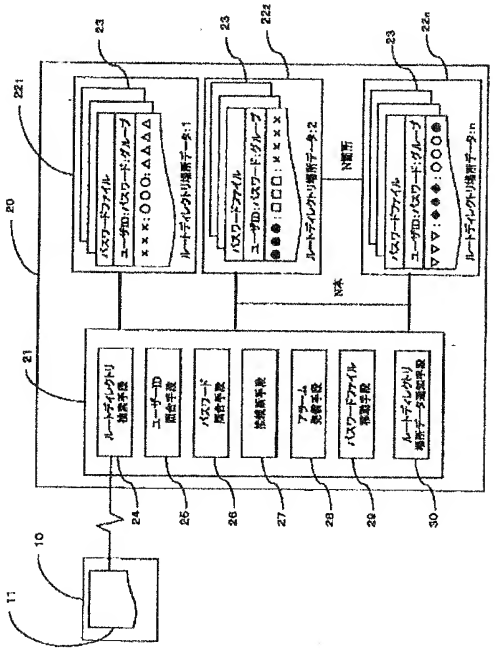
(22)出願日　平成11年３月12日(1999.3.12)

(71)出願人　000232047
日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号
(72)発明者　新川　仁彦
東京都港区芝浦三丁目18番21号　日本電気エンジニアリング株式会社内
(74)代理人　100106563
弁理士　中井　潤

Ｆターム(参考)　5B017 AA01 AA04 BA05 BA07 BA10
BB02 BB07 BB09 CA16
5B085 AE03 AE08 BG07
5B089 GA11 GA21 JB22 KA17 KB13
KC44 KC58 KG10

(54)【発明の名称】　パスワード認証方法及びパスワード認証システム

(57)【要約】
【課題】　情報ネットワーク通信システムにおいて、パスワードを第三者に盗まれても、第三者による情報通信ネットワークシステムへの不正侵入を阻止する。
【解決手段】　サーバー２０内に、ユーザー毎のパスワードファイル２３を格納するための複数箇所のルートディレクトリ22_1～22_nを用意し、アクセス時にユーザーＩＤ、パスワード及びパスワードファイル２３を格納したルートディレクトリの場所データとをサーバー２０に送信し、該当するルートディレクトリのパスワードファイル２３に記録されたパスワードが一致したときにサーバー２０へのログインを許可するとともに、ログアウト時にはパスワードファイル２３を格納したルートディレクトリをそれまで格納していたルートディレクトリからそれ以外のルートディレクトリにランダムに場所移動し、該場所移動したルートディレクトリの場所データをアクセス端末１０の記憶部１１に記憶する。



1

【特許請求の範囲】

【請求項１】　サーバーと、該サーバーに通信回線を介して接続される複数のアクセス端末とで構成される情報通信ネットワークシステムにおいて、

前記サーバー内に、ユーザーＩＤとパスワードを記録するためのパスワードファイルを各ユーザー毎に用意するとともに、これらパスワードファイルを格納するための複数箇所のルートディレクトリを用意し、

サーバーへのアクセス時に、アクセス端末から自己のユーザーＩＤと、パスワードと、これらユーザーＩＤとパスワードを記録したパスワードファイルを格納したルートディレクトリの場所データとをサーバーに送信し、

該当するルートディレクトリのパスワードファイルに記録されたパスワードがアクセス端末から送られてきたパスワードと一致したときにサーバーへのログインを許可するとともに、

ログアウト時にはパスワードファイルをそれまで格納していたルートディレクトリからそれ以外のルートディレクトリにランダムに場所移動し、

該変更したルートディレクトリの場所データを対応するアクセス端末に送信してアクセス端末内に記憶することを特徴とするパスワード認証方法。

【請求項２】　サーバーと、該サーバーに通信回線を介して接続される複数のアクセス端末とで構成される情報通信ネットワークシステムにおいて、

前記各アクセス端末に、

前記サーバーから送られてくる自己のパスワードファイルについてのルートディレクトリの場所データを格納記憶する記憶部を備えるとともに、

前記サーバー内には、

各ユーザー毎に用意したユーザーＩＤとパスワードを記録するためのパスワードファイルを格納する複数箇所のルートディレクトリと、

アクセス端末から送信されるルートディレクトリの場所データに対応したルートディレクトリを検索するルートディレクトリ検索手段と、

アクセス端末から送信されたユーザＩＤに対応するパスワードファイルが前記ルートディレクトリ検索手段によって検索されたルートディレクトリ内に存在するか否かを照合するユーザーＩＤ照合手段と、

アクセス端末から送信されたパスワードが前記ユーザーＩＤ照合手段で選択されたパスワードファイルに記録されたパスワードと一致するか否かを照合するパスワード照合手段と、

少なくともアクセス端末から前記ルートディレクトリの場所データが送信されてこない場合には通信回線を自動的に切断する接続断手段と、

アクセス端末からサーバーにログインした正規ユーザーのログアウト時に、パスワードファイルをそれまで格納していたルートディレクトリからそれ以外の他のルートディレクトリにランダムに場所移動するパスワードファイル移動手段と、

該パスワードファイル移動手段によって変更されたルートディレクトリの場所データを対応するアクセス端末に向けて送信するルートディレクトリ場所データ通知手段とを備えたことを特徴とするパスワード認証システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、サーバーと、該サーバーに通信回線を介して接続される複数のアクセス端末とで構成される情報通信ネットワークシステムにおいて、サーバーへの不正侵入を阻止し、セキュリティの強化を図るためのパスワード認証方法とパスワード認証システムに関する。

【０００２】

【従来の技術】セキュリティを考慮した情報通信ネットワークシステムにログインする場合には、正規のユーザーであるかどうかを認証するために、情報通信ネットワークシステムのサーバーはアクセス端末に対してパスワードの入力を要求する。そして、ログインしようとするユーザーは、予めサーバーに登録しておいた文字列からなるパスワードをアクセス端末のキーボードから入力する。情報通信ネットワークシステムのサーバーは、この入力された文字列と予め登録されている文字列とが一致するか否かをユーザーＩＤとパスワードを記録したパスワードファイルにアクセスして判定し、一致すれば本人であると認証してログインを許可する。

【０００３】サーバー内では、パスワードファイルは符号化・暗号化されて格納されているが、セキュリティの上では、各ユーザーが採用する生のパスワード自体も第三者に容易に推測されないものであることが望ましい。しかしながら、一般に全く意味のない文字や数字はパスワードとして覚えるのが大変であるため、多くのユーザーは辞書に載っている単語や自分の生年月日あるいは電話番号等、身近で第三者が簡単に推測できる単純な文字列をパスワードにしてしまうことが多い。また、たとえ簡単に推測できないようなパスワードを採用したとしても、第三者の前でキーボードからパスワードを入力するような場合には、入力する手の動きから第三者にパスワードを知られることがある。

【０００４】さらに、パスワードファイルは符号化・暗号化されているものの、通常、全てのユーザーのパスワードファイルを１ヶ所のルートディレクトリにまとめて格納しているため、正規ユーザーでない第三者が何らかの方法で通信ネットワークシステムに不正侵入した場合、全てのユーザーについての全てのパスワードを盗むことが可能となり、リモートで情報通信ネットワークシステムに対して不正な侵入を容易に許してしまうおそれがある。

【０００５】

証システムの実施の形態の具体例を図面を参照しながら説明する。

【００１３】図１は、本発明にかかるパスワード認証システムの第１実施例を示すブロック図である。ネットワークのアクセス端末１０は、ルートディレクトリ場所データを格納するための記憶部１１を備え、情報通信ネットワークシステムの中核をなすサーバー２０は、中央処理制御部２１と、複数（ｎ箇所）のルートディレクトリと、各ルートディレクトリ22_1～22_nに分散格納されたユーザー単位ごとのパスワードファイル２３を備える。

【００１４】前記中央処理制御部２１は、ルートディレクトリ検索手段２４と、ユーザーＩＤ照合手段２５と、パスワード照合手段２６と、接続断手段２７と、アラーム発信手段２８と、パスワードファイル移動手段２９と、ルートディレクトリ場所データ通知手段３０とで構成されている。尚、中央処理制御部２１は、ＣＰＵやメモリ等によって構成されており、各手段２４～３０は中央処理制御部２１内に格納された制御処理プログラムによってソフトウェア的に実現されている。

【００１５】図２は、前記パスワード認証システムにおけるパスワードの認証動作の処理手順を示すフローチャートである。この図２を参照して、図１のパスワード認証システムのパスワード認証動作について説明する。

【００１６】本発明のパスワード認証システムは、予め、初期設定として各ユーザー毎にパスワードファイル２３を作成し、このユーザー毎のパスワードファイル２３に各々のユーザーＩＤとパスワードを記録した上で、各々のパスワードファイル２３をサーバー２０内のｎ箇所のルートディレクトリ22_1～22_nに分散格納するとともに、各アクセス端末１０の記憶部１１に、自己のパスワードファイル２３を格納したルートディレクトリ22_1～22_nの場所データを格納記録しておく。

【００１７】正規ユーザーが自己のアクセス端末１０を通じて情報通信ネットワークシステムのサーバー２０にログインする場合には、アクセス端末１０のキーボードよりユーザーＩＤを入力し、サーバー２０に送信する（図２のステップＳ３１）。アクセス端末１０は、このユーザＩＤの送信に併せて、予め記憶部１１に格納しておいたルートディレクトリの場所データもサーバー２０の中央処理制御部２１に送信する（図２のステップＳ３２）。

【００１８】サーバー２０内の中央処理制御部２１は、ルートディレクトリ検索手段２４とユーザーＩＤ照合手段２５とによって、前記送信されてきたルートディレクトリの場所データからルートディレクトリ22_1～22_n内の該当するルートディレクトリを選択し、該ルートディレクトリ内にユーザーＩＤに対応するパスワードファイルが存在するか否かを検索する（図２のステップＳ３３）。そして、対応するユーザーＩＤに対応するパスワードファイルが存在する場合には、アクセス端末１０に対してパスワードの入力を促す。

【００１９】正規ユーザーはアクセス端末１０のキーボードよりパスワードを入力し、サーバー２０の中央処理制御部２１に送信する（図２のステップＳ３４）。中央処理制御部２１のパスワード照合手段２６は、前記検索されたルートディレクトリのパスワードファイル２３に格納されているパスワードと、前記送信されてきたパスワードとの照合を行ない（図２のステップＳ３５）、一致していれば正規ユーザーに対してサーバー２０へのログインを許可する（図２のステップＳ３６）。これによって、ログインした正規ユーザーは所望の処理を実行する。

【００２０】そして、サーバー２０にログインした前記正規ユーザーが所望の処理を終了し、サーバー２０からログアウトする際には（図２のステップＳ４１）、中央処理制御部２１のパスワードファイル移動手段２９は、前記正規ユーザーのユーザーＩＤとパスワードを格納したパスワードファイル２３をｎ箇所あるルートディレクトリ22_1～22_nのうち、それまで格納していたルートディレクトリからそれ以外の他のルートディレクトリに乱数等を利用してランダムに移動させる（図２のステップＳ４２）。

【００２１】パスワードファイル２３を移動したルートディレクトリの場所データは、中央処理制御部２１のルートディレクトリ場所データ通知手段３０を通じて対応するアクセス端末１０の記憶部１１に送信され（図２のステップＳ４３）、アクセス端末１０内の記憶部１１に記憶されているルートディレクトリの場所データを新しい場所データに書き換える（図２のステップＳ４４）。

【００２２】正規ユーザーが再度ログインする際には、前回のログアウト時に記憶部１１に格納した新しいルートディレクトリの場所データに基づき、上記したと同様にしてパスワードの認証を行う（図２のステップＳ３１）。従って、正常なアクセスを行なっている限り、正規ユーザーは何らの規制を受けることなくその都度サーバー２０へログインすることができる。

【００２３】次に、正規ユーザーでない第三者がパスワードを何らかの方法で盗み出し、該パスワードを用いてリモートから情報通信ネットワークシステムのサーバ２０への不正侵入を試みた場合のパスワード認証動作について説明する。

【００２４】情報通信ネットワークシステムのサーバー２０へ侵入する際、正規ユーザーでない第三者が盗み出したユーザーＩＤを入力すると（図２のステップＳ３１）、この入力されたユーザーＩＤは情報通信ネットワークシステムのサーバー２０へ送信される（図２のステップＳ３２）。

【００２５】しかしながら、入力したユーザーＩＤとこれに対応したパスワードを記録したパスワードファイル

２３が複数箇所のルートディレクトリ２２$_1$～２２$_n$中のどのルートディレクトリにあるかということを示す場所データが送信されないため、中央処理制御部２１のルートディレクトリ検索手段２４とユーザーＩＤ照合手段２５は、パスワードを検索して一致しているかどうかの判断を行なうことができない（図２のステップＳ３３）。従って、サーバー２０は、不正なアクセスであるとして、この正規ユーザーでない第三者のログインを許可しない（図２のステップＳ３７）。

【００２６】また、初期設定時のルートディレクトリの場所データを正規ユーザーでない第三者が知っていたとしても、正規ユーザーがサーバー２０にログイン・ログアウトする毎に、正規ユーザーのユーザーＩＤに対応したパスワードファイル２３がランダムにルートディレクトリ２２$_1$～２２$_n$を移動するので、正規ユーザーでない第三者が現時点におけるユーザーＩＤに対応したパスワードファイル２３のルートディレクトリ２２$_1$～２２$_n$の場所データを入手して不正侵入することは不可能である。

【００２７】正規ユーザーでない第三者が前記パスワードファイル２３をランダムに格納するための全てのルートディレクトリ２２$_1$～２２$_n$の場所を知り得た場合には、正規ユーザーでない第三者が情報通信ネットワークシステムのサーバー２０へ侵入する確率は、前記ルートディレクトリ２２$_1$～２２$_n$の場所数ｎに対応し、１／ｎとなる。従って、確率上ではｎ回の試行により情報通信ネットワークシステムのサーバー２０へ不正侵入されることになるが、最初の侵入の際にルートディレクトリ２２$_1$～２２$_n$の場所を間違った時点で、中央処理制御部２１の接続断手段２７によって当該接続回線を強制的に切断し（図２のステップＳ３７）、アラーム発信手段２８から管理者及び正規ユーザーに対してアラームを発信し、不正侵入が発生したことを知らせるとともに、正規ユーザーにパスワードを変更するように促す（図２のステップＳ３８）。これによって、正規ユーザーでない第三者がｎ回の試行をしても不正侵入することができなくなり、情報通信ネットワークシステムのセキュリティを高めることができる。

【００２８】次に、本発明にかかるパスワード認証システムの第２実施例について、図３を参照して説明する。尚、図３中、前記第１実施例（図１）と同一または相当部分には同一の符号を付し、その詳細な説明は省略する。

【００２９】この第２実施例にかかるパスワード認証システムは、制御処理プログラムを記録した記録媒体３１を外部に、制御処理プログラムを入れ換え自在とした点で前記第１実施例のものと異なるだけである。尚、記録媒体３１としては、磁気ディスク、半導体メモリ、その他の記録媒体を利用することができる。

【００３０】記録媒体３１の制御処理プログラムは、記録媒体３１から中央処理制御部２１に読み込まれ、中央処理制御部２１は前記第１実施例における中央処理制御部２１による処理と同じ処理を実行する。

【００３１】すなわち、アクセス端末１０より、ユーザーＩＤとルートディレクトリ場所データが与えられると、中央処理制御部２１は、まずルートディレクトリ場所データに基づき、ルートディレクトリ２２$_1$～２２$_n$中の指定のルートディレクトリを検索し、ユーザーＩＤの照合を行う。該照合処理の結果、当該ルートディレクトリにユーザーＩＤが存在する場合には、パスワードの入力をアクセス端末１０に促し、前述した第１実施例と同様にパスワードを照合し、パスワードが一致する場合にはサーバー２０へのログインを許可する。

【００３２】一方、前記照合処理の結果、該当するルートディレクトリにユーザーＩＤが存在しない場合には、前記アクセス端末１０との接続を断ち、管理者及び正規ユーザーにアラームを発信し、不正侵入が発生したことを知らせるとともに、正規ユーザーにパスワードを変更するように促す。

【００３３】サーバー２０にログインした正規ユーザーが、サーバー２０からログアウトする際には、中央処理制御部２１は、前記正規ユーザーのユーザーＩＤとパスワードを格納したパスワードファイル２３をｎ箇所あるルートディレクトリ２２$_1$～２２$_n$のうち、それまで格納していたルートディレクトリからそれ以外の他のルートディレクトリにランダムに移動させ、この移動させたルートディレクトリの場所データをアクセス端末１０に送信する。これによって、前記第１実施例と同様に、第三者による不正侵入を阻止することができる。

【００３４】

【発明の効果】以上説明したように、本発明のパスワード認証方法とパスワード認証システムによれば、パスワードファイルへのルートディレクトリが複数箇所あるため、パスワードの入力だけではなく、パスワードファイルの存在するルートディレクトリの場所を指定する場所データがなければ、情報通信ネットワークシステムに侵入することができず、さらに、ログアウトごとにランダムにパスワードファイルを格納するルートディレクトリが変わるため、パスワードファイルが格納されているルートディレクトリの場所データを正規ユーザーでない第三者が手に入れることは困難となる。このため、たとえ推測や盗み見等によってパスワードを見破られたとしても、容易にネットワークへ侵入できないようにすることができ、情報通信ネットワークシステムにおけるセキュリティを格段に向上させることができる。

【００３５】また、ユーザーごとのパスワードファイルを複数箇所のルートディレクトリに分散して格納することにより、全てのユーザーのパスワードを知るためには複数箇所のルートディレクトリを調べなければならず、たとえ何らかの方法で不正侵入できたとしても、複数箇

所のルートディレクトリの存在場所を知らない限り、全てのユーザーのパスワードを盗むことができなくなり、情報通信ネットワークシステムにおけるセキュリティを格段に向上させることができる。

【図面の簡単な説明】

【図１】本発明にかかるパスワード認証システムの第１実施例を示すブロック図である。

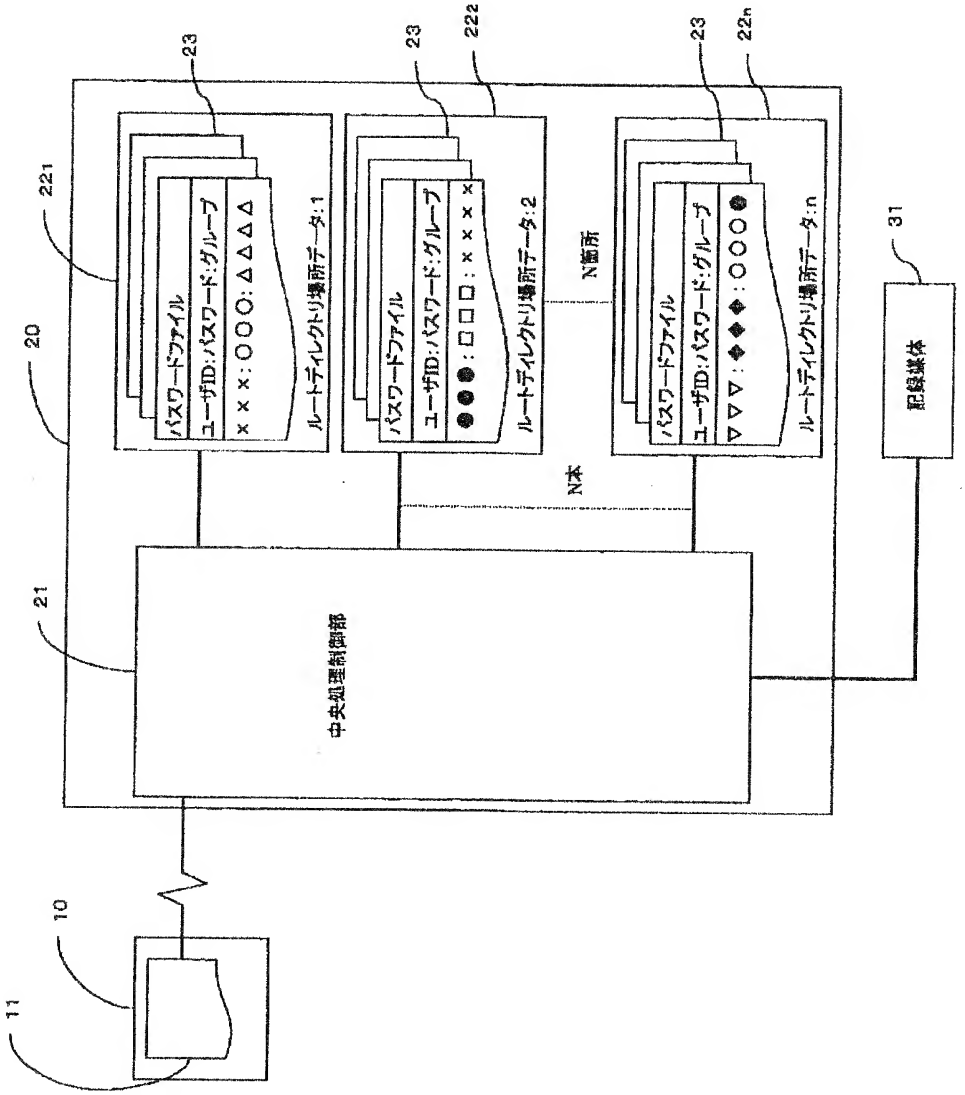
【図２】図１のパスワード認証システムによる処理手順を示すフローチャートである。

【図３】本発明にかかるパスワード認証システムの第２実施例を示すブロック図である。

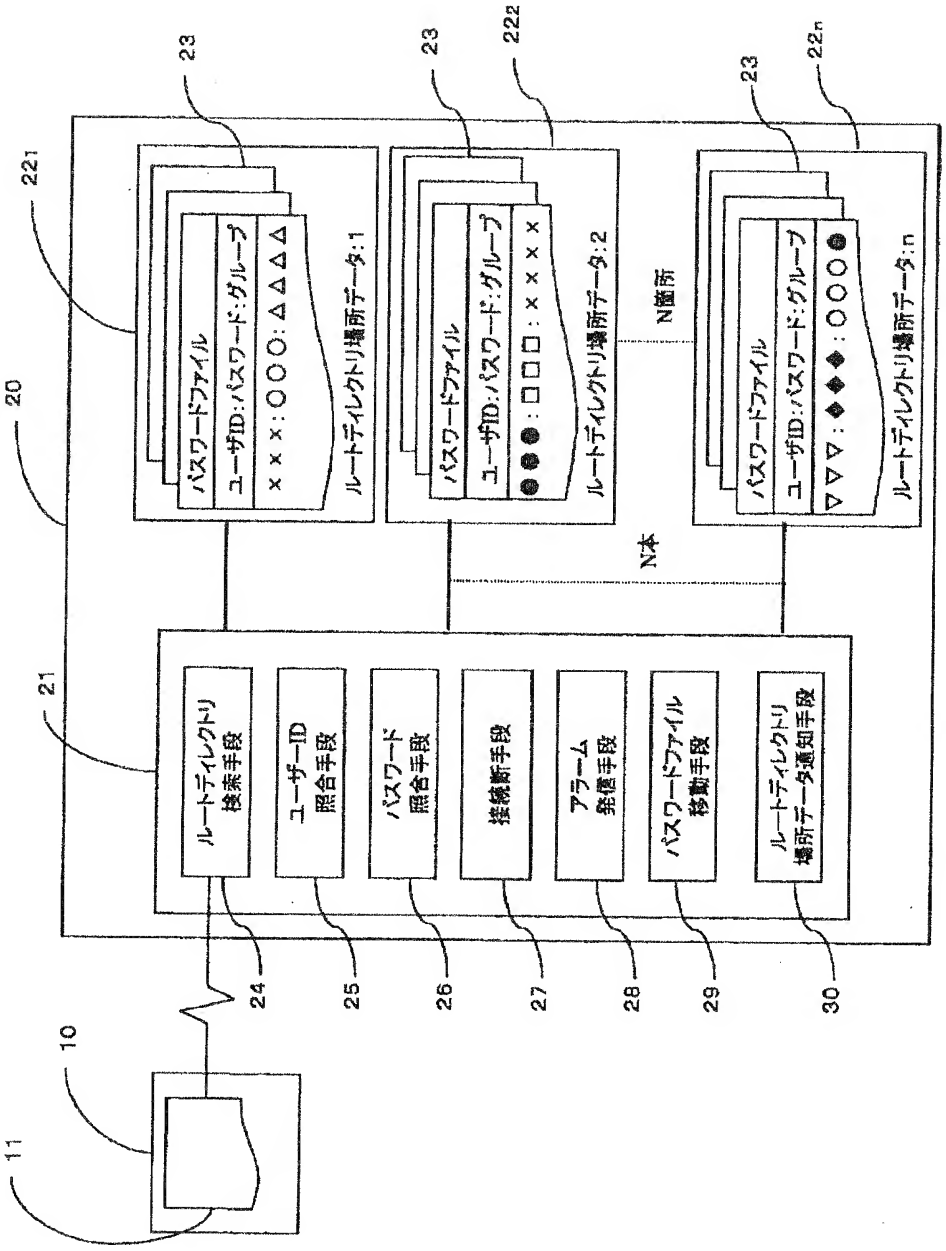
【符号の説明】

１０　　アクセス端末
１１　　記憶部
２０　　サーバー
２１　　中央処理制御部
22_1～22_n　　ルートディレクトリ
２３　　パスワードファイル
２４　　ルートディレクトリ検索手段
２５　　ユーザーＩＤ照合手段
２６　　パスワード照合手段
２７　　接続断手段
２８　　アラーム発信手段
２９　　パスワードファイル移動手段
３０　　ルートディレクトリ場所データ通知手段
３１　　記録媒体

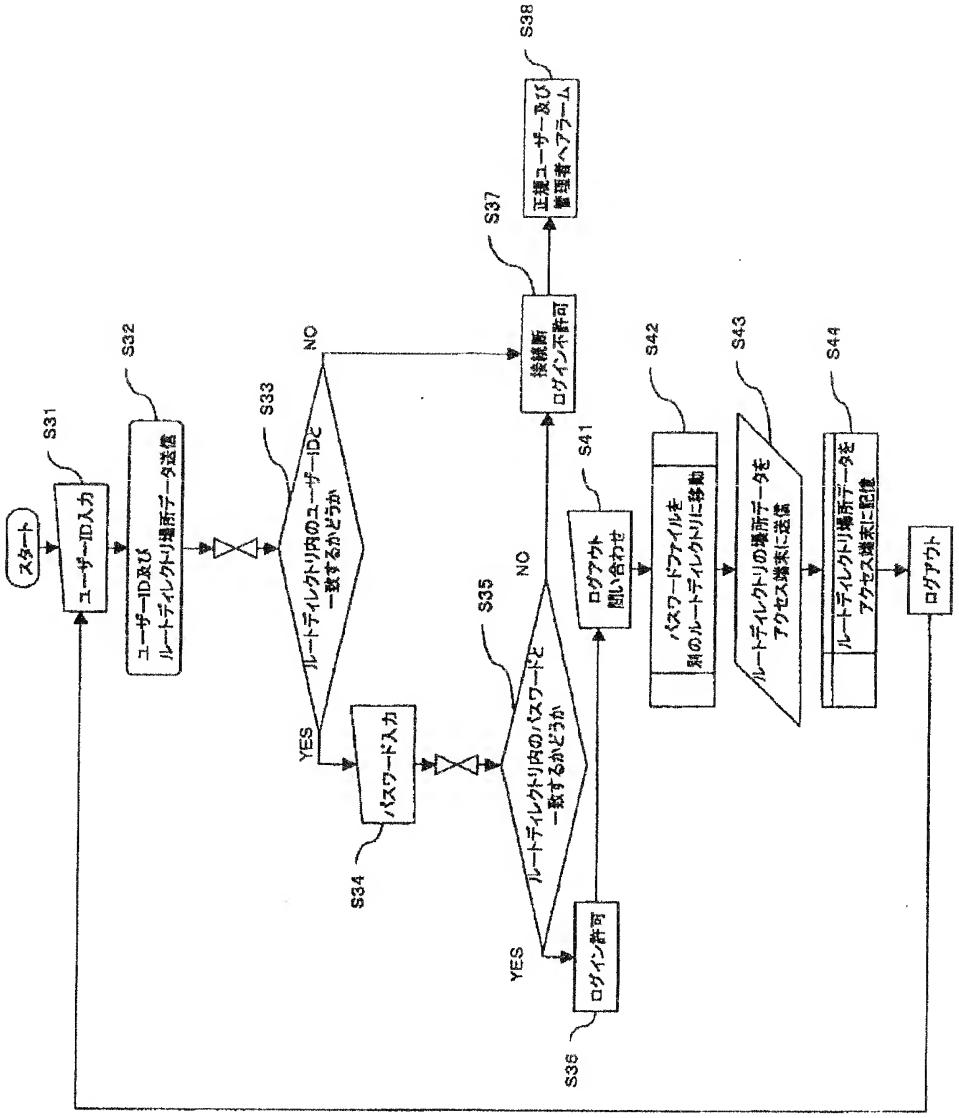
【図３】



【図１】


20
21
221
222
22n
23
パスワードファイル
ユーザID:パスワード:グループ
×××:○○○:△△△△
ルートディレクトリ場所データ:1
●●:□□□:××××
ルートディレクトリ場所データ:2
▽▽▽:◆◆◆:○○○●
ルートディレクトリ場所データ:n
N箇所
N本
ルートディレクトリ検索手段
ユーザーID照合手段
パスワード照合手段
接続断手段
アラーム発信手段
パスワードファイル移動手段
ルートディレクトリ場所データ通知手段
24
25
26
27
28
29
30
10
11

【図２】


スタート
S31
ユーザーID入力
S32
ユーザーID及び
ルートディレクトリ場所データ送信
S33
ルートディレクトリ内のユーザーIDと
一致するかどうか
NO
YES
S34
パスワード入力
S35
ルートディレクトリ内のパスワードと
一致するかどうか
NO
YES
S36
ログイン許可
S37
接続断
ログイン不許可
S38
正規ユーザー及び
管理者へアラーム
S41
ログアウト
問い合わせ
S42
パスワードファイルを
別のルートディレクトリに移動
S43
ルートディレクトリの場所データを
アクセス端末に送信
S44
ルートディレクトリ場所データを
アクセス端末に記憶
ログアウト